

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))INFORMATION ASSOCIATED WITH APPLE ACCOUNT)
AHMADABDULLAHMALMAHDI@ICLOUD.COM THAT IS)
STORED AT PREMISES CONTROLLED BY APPLE INC.)

Case No. 25-870M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

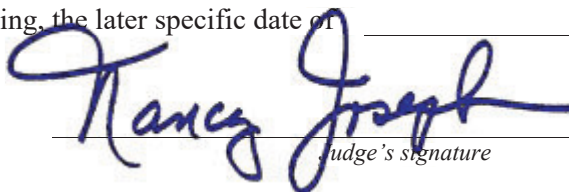
Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before March 21, 2025 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: March 7, 2025 @ 3:30 p.m.City and state: Milwaukee, Wisconsin
Judge's signatureHonorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Apple account and iCloud account with username: ahmadabdullahmahdi@icloud.com, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered in Cupertino, CA.

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any emails, messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) February 21, 2025, Apple is required to disclose the following information to the government for each account listed in Attachment A:

a. The contents of all emails associated with the account from since account creation to current date, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

b. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

c. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple

and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

d. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

e. All records pertaining to the types of service used;

f. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §245(b)(2): Federally Protected Activities; 18 U.S.C. §875 (c): Interstate Threats; and 18 U.S.C. §1038(a): False Information and Hoaxes those violations involving Zidan Abdallah and occurring after August 1, 2024, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

A. Communications between the user of the SUBJECT ACCOUNT and victims;

B. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

C. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

D. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such persons(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH APPLE ACCOUNT
AHMADABDULLAHALMAHDI@ICLOUD.COM THAT IS
STORED AT PREMISES CONTROLLED BY APPLE INC.

Case
No.25-870M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Please see Attachment A.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §245(b)(2)	Federally Protected Activities
18 U.S.C. §875(c)	Interference with commerce by threats or violence
18 U.S.C. §1038(a)	False information and hoaxes

The application is based on these facts:

Please see Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

AMY MENTZEL

Digitally signed by AMY MENTZEL
Date: 2025.03.06 10:07:00 -06'00'

Applicant's signature

Amy Mentzel, Special Agent - FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____
telephone _____ (specify reliable electronic means).

Date: 3/7/2025

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AN APPLICATION FOR A SEARCH WARRANT

I, Amy Mentzel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account, that is stored at premises owned, maintained, controlled, or operated by Apple, a cloud storage provider headquartered at Apple Inc., a company headquartered in Cupertino, CA. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent for the Federal Bureau of Investigation (“FBI”), where I have been employed since 2006. I am currently assigned to an FBI squad which investigates civil rights and public corruption crimes. I was previously assigned to FBI Human Trafficking and Crimes Against Children Task Forces in the FBI Milwaukee and Detroit Divisions. I primarily investigated human trafficking, child exploitation, and kidnapping cases.

3. I am a federal law enforcement officer under applicable provisions of the United States Code and under Rule 41(a) of the Rules of Criminal Procedure. I have received training and have experience in the enforcement of the laws of the United States, including preparation and presentation of search warrants, and in executing court-ordered search warrants.

4. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. The facts set

forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary for the limited purpose of establishing probable cause to conduct a search of and for the items described in Attachments A and B for evidence, contraband, and/or instrumentalities of the criminal conduct described herein. Additionally, unless otherwise indicated, wherever in this Affidavit I assert that an individual made a statement, that statement is described in substance herein and is not intended to be a verbatim recitation of such statement. Furthermore, unless otherwise indicated, all statements contained in this Affidavit are summaries in substance and in part. The following is true to the best of my knowledge and belief.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §245(b)(2): Federally Protected Activities, 18 U.S.C. §875 (c): Interstate Threats, and 18 U.S.C. §1038(a): False Information and Hoaxes, have been committed, are being committed, or will be committed by Zidan Abdallah. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i) AND/OR is in . . . a district in which the provider . . . "is located or in which the wire or electronic communications, records, or other information are stored.” 18 U.S.C. § 2711(3)(A)(ii).

TECHNICAL TERMS

7. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

8. Instant messaging (IM) is a collection of technologies that create the possibility of real-time text-based communication between two or more participants via the Internet. Instant messaging allows for the immediate transmission of communications, including immediate receipt of acknowledgment or reply.

9. The term “Internet” is defined as the worldwide network of computers, a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider (“ISP”), which operates a host computer with direct access to the Internet.

10. The term “ISP” (Internet Service Provider), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

11. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like

a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

12. Log files are computer files containing information regarding the activities of computer users, processes/programs running on the system and the activity of computer resources such as networks, modems, and printers. Log files can be used to identify activities that occurred on a specific computer. Installation (or install or setup) of a program is the act and the effect of putting the program in a computer system so that it can be executed.

PROVIDER BACKGROUND

13. Apple is a United States company that designs, manufactures, and markets mobile communication and media devices, personal computers, and portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod, Apple TV, a portfolio of consumer and professional software applications, the iOS and Mac OS X operating systems, iCloud, and a variety of accessory, service and support offerings. Apple also sells and delivers digital content and applications through the iTunes Store, App Store, iBookstore, and MacApp Store.

14. The iPhone is a line of smartphones designed and marketed by Apple. It runs Apple's iOS mobile operating system. The user interface is built around the iPhone's multi-touch screen, including a virtual keyboard. The iPhone has wireless internet capabilities and can connect to many cellular networks around the world. The iPhone can shoot video, send and receive email, browse the Internet, send text messages, provide navigation services via Global Positioning Satellite location technology, record notes, do mathematical calculations, and receive visual and audio voicemail. Other functions such as video games, reference works, social networking—

including Facebook and Twitter—can be enabled by downloading application programs (“apps” or, singular, “app”). Apple operates an App Store which offers numerous apps by Apple and third parties.

15. The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Manage and use your Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “Introduction to iCloud,” available at <https://support.apple.com/kb/PH26502>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; and “Apple Platform Security,” available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

16. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.
- c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on

any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
- e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

- f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.
- g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

17. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

18. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means

of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

19. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “capability query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the “Find My” service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

20. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a

user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

21. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

22. The following additional information may be available from Apple:

- a. *Subscriber Information.* When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud subscriber information

and connection logs with Internet Protocol (“IP”) addresses can be obtained with a subpoena or greater legal process.

- b. *Mail Logs.* Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses.
- c. *Email Content.* iCloud stores the email a subscriber has elected to maintain in the account while the subscriber’s account remains active.
- d. *Device Information.* Apple maintains information regarding the types and identities of devices used to access iCloud accounts, including mobile telephones, computer tablets, laptop and desktop computers, and other computing devices.
- e. *Other iCloud Content. Photo Stream, Docs, Contacts, Calendars, Bookmarks, iOS, Device Backups, and Encryption Keys.* iCloud stores content for the services that the subscriber has elected to maintain in the account while the subscriber’s account remains active. Apple does not retain deleted content once it is cleared from Apple’s servers. iCloud content may include stored photos, documents, contacts, calendars, bookmarks and iOS device backups. iOS device backups may include photos and videos in the users’ camera roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. iCloud backups for all operating systems are encrypted by default. However, an iCloud account may include encryption keys – contained in “keybag” and “FileInfoList.txt” files – enabling law enforcement to decrypt the contents of these backups.
- f. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email

accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- g. *Game Center*. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
- h. *Historical geolocation data*. Apple stores information regarding the historical location of iPhone and other Apple devices associated with iCloud accounts;
- i. *Find My iPhone and Remote Deletion Activity*: Find My iPhone is a user-enabled feature by which an iCloud subscriber is able to locate his/her lost or misplaced iPhone, iPad, iPod touch or Mac and/or take certain actions, including putting the device in lost mode, locking or wiping the device.
- j. *App Store and iTunes Store*. These are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music,

movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

- k. *iPhone Dev Center and Apple Developer*. These services allow users to develop software and computer code for Apple platforms, including iPhone apps.
- l. *Preserved Data*. Apple typically maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

PROBABLE CAUSE

23. On December 23, 2024, security personnel at the University School of Milwaukee (USM), located in River Hills, Wisconsin, contacted the River Hills Police Department (RHPD) to report USM had received a bomb threat from telephone number 587-205-6694. RHPD determined 587-205-6694 to be a “spoof” or fake number. USM was on holiday break, but hockey games were scheduled to take place on school grounds that day. USM security guard, J.P., told officers with RHPD that the caller asked if he was speaking with USM, and he stated he was going to blow up the school.

24. The caller asked if J.P. was a devil worshipper and stated he would destroy the school, and that he would blow up the school. The caller made comments about Christians and Jews and other statements related to religion. The bomb threat prompted USM to contact RHPD, and the school was “shut down.”

23. J.P. also advised RHPD that a threatening voicemail had been left with USM from 917-686-2997 on December 21, 2024.

24. RHPD found 917-686-2997 to be associated with Zidan Wesam ABDALLAH in Franklin Police Department (FPD) and Mequon Police Department (MPD) reports. This phone number was also attributed to ABDALLAH in police reports obtained from the University of California, Santa Barbara Police Department (UCSB). On December 22, 2024, ABDALLAH's father contacted UCSB stating that ABDALLAH had left him a voicemail from this number threatening to kill him.

25. On December 24, 2024, USM contacted RHPD to advise that another threatening voicemail to USM was found from 414-415-4374, a number that was not attributed to a caller or carrier.

26. ABDALLAH had been a student at USM, but he had been expelled due to behavior issues.

27. J.P. provided your Affiant with the two recorded voicemails to USM from telephone numbers 917-686-2997 and 414-415-4374. In one of the voicemails, the caller identifies himself as ABDALLAH.

VOICEMAIL 1: DECEMBER 21, 2024, FROM 917-686-2997

28. The following is a synopsis of the December 21, 2024, voicemail left for a USM employee. (Unintelligible ("UI")) My name is Zidan Wesam (UI) Abdallah. I (UI) over you, I'm, I'm the (UI), I'm the caliph of this world, I've been with spiritual energy in this world. Your ps-your school, I'm de..I'm publicly declaring under God, your school is pathetic, its satanism, its Jewi-Judaism, you guys are all bought and known, pathetic white people, soulless white people, that think they have any spiritual energy or power. You guys are all pathetic and useless. You guys understand you're my bitches. I'll step on you like my fucking end of my fucking shoe. You understand me? Whoever is listening to this fucking, uh-uh, call. I dare you to challenge me. I dare

you to go against me, you fucking pussy. You fucking little bitch, (UI), you-you fucking cowards. You guys were so scared of people that you-you, powered in your own school and made your own secret organization. You fucking idiots. You pathetic fucking, you mother fuckers, you guys literally fuck your own mothers and masturbate to your children, you pedophilic, satanistic, disgusting mother fuckers, you disgusting bitches, disgusting Jewish b-bitches. Fuck you niggas bro. Dead ass, fuck you niggas, you niggas are fucking retarded as fuck, you niggas are fucking slow. You niggas think your smart brain beats (UI) making (UI). All right bro, let see what God's about to do to your dumb ass school you bitch ass niggas. You pussy ass niggas, fuck you bitch ass niggas. Fuck you, suck my dick, bitch. Literally, (UI) literally, suck it, just like you suck your own Dad's dick, most of you, fucking pussys, literally, fuck you niggas.

VOICEMAIL 2: DECEMBER 23, 2024, FROM 414-415-4374

29. The following is a synopsis of the December 23, 2024, voicemail left for a USM employee. You guys are all going to be ravaged. You guys are all going to be torn to bits like the animals you are. You fucking sick savages. Fuck you all. You fucking, stupid mother fuckers. You fucking animals, you demons. I am living proof that the devil has no power. If I, for this guy that just recorded this voicemail. If I took his mom and I fucked his mom, with um, a sword and then I killed her (UI) and chopped her head off. What would you do? What would you do? Mother fucker. Fucking pussys. You guys know exactly who I am. You guys know exactly who you fucked with. You guys know exactly what your about to get up your fucking asses, all of you.

STATEMENTS FROM A.F. AND M.J.

30. On January 6, 2025, A.F. contacted the Milwaukee FBI to advise that Instagram user "ahmadabdullahalmahdi" had posted videos or "stories" to Instagram threatening Jewish students and an Indian student. The poster, who appears in many of the videos was identified by

USM students and parents as ABDALLAH. A.F. advised that in the videos, ABDALLAH stated, “I hate Jews so much I’m going to kill them all,” and “we need to kill all the Jews.”

31. Your Affiant reviewed the videos provided by A.F. In one of the videos, ABDALLAH threatens to rip the head off M.J. and calls her a “disgusting, evil Indian.” He states several times in the video that he will kill M.J. and if he sees her, he will “have to take her life.” In another video ABDALLAH vehemently states “It’s time for the Jews to die and the Indians to die.”

32. On January 6, 2025, M.J. contacted the UC Santa Barbara Police Department (“UCSB”) to report that she received direct messages from “ahmadabdullahalmahdi” via Instagram Messenger, who M.J. knew to be ABDALLAH. The police report states ABDALLAH messaged, “I’m going to kill you...You will die...Indian.” ABDALLAH also posted a video to the Instagram account stating he would “slice your fucking head off your body” and called M.J. an “Indian slut.” M.J. told an officer that she had attended school with ABDALLAH at USM, but they were not friends and did not really know each other. ABDALLAH made at least four videos posted on Instagram threatening to kill M.J. On January 6, 2025, ABDALLAH was served with an Emergency Protective Order (“EPO”) for M.J. When served with the order, ABDALLAH stated to the officer, “It doesn’t matter either because if she’s gonna be killed she’s gonna be killed with me and my army.” The officer noted that a later Instagram story on ABDALLAH’s account contained a video of the EPO torn into pieces. On Monday, January 6, 2025, UCSB arrested ABDALLAH for state violations of criminal trespass and stalking.

OTHER THREATS FROM 917-686-2997 AND INSTAGRAM

33. A UCSB missing person report for ABDALLAH, dated December 18, 2024, listed 917-686-2997, as the contact number for ABDALLAH. The report was made by ABDALLAH’s

father, who resides in Wisconsin. ABDALLAH's father made the report after ABDALLAH had not contacted his father for several hours after sending threatening text messages to his father and other family members. An additional December 18, 2024, UCSB report stated that these text messages to ABDALLAH's father and family members were sent between December 16 and December 18, 2024, and included, "I'm going to rape and destroy you," "Either serve me or die," and "If you do not serve me, its time for you to die."

34. A Santa Barbara County Sheriff's Department (SBCSD) report dated December 23, 2024, also associates phone number 917-686-2997 with ABDALLAH. ABDALLAH was arrested for vandalism and the assault of a security guard at a marijuana dispensary in Isla Vista, California.

35. On January 6, 2025, former USM student, H.L., made a complaint to the Mequon Police Department (MPD) regarding threats by ABDALLAH. H.L. stated that ABDALLAH made threats to H.L. and others, on Instagram stories. In a video, ABDALLAH stated, "Keep in mind that [H.L.'s first and last name] already knows he is going to die, he already knows I'm gonna kill him. He's gonna bow to me and he is gonna die." The MPD report also stated that ABDALLAH posted images showing his admiration for Luigi Mangione, who is a suspect criminally charged in a homicide in an allegedly planned assassination.

36. A compilation of numerous ABDALLAH Instagram videos and postings from USM parents was provided by USM on January 16, 2025. The videos were identified by USM and parents of USM students, after USM sent notification emails to the parents after the December 23, 2024, bomb threat. Your Affiant has viewed recent booking photos from California of ABDALLAH, and ABDALLAH does appear in numerous undated videos in which he references killing Jews and crucifying "so many of you." There is a photo of four female USM students, and the three who are known to be Jewish have their faces crossed out with the word "Death" above

them. In one video ABDALLAH states that anyone who challenges him will be killed. “I have to kill you. I have to kill somebody. Somebody has to die.” ABDALLAH stated, “We need to kill all the Jews so I can get to Heaven.” In other videos ABDALLAH stated he will masturbate to people dying and Jews dying. ABDALLAH mentions several USM students who are Jewish and threatens to kill them.

HARASSMENT OF MINOR 1 THROUGH APPLE iMESSAGE

37. On August 21, 2024, an acquaintance of ABDALLAH’s, MINOR 1, reported to law enforcement that she had received hundreds of iMessages from ABDALLAH, after MINOR 1 discontinued their relationship on or about August 19, 2024. The police report indicates that on between August 19, 2024, and August 21, 2024, ABDALLAH sent approximately 542 Apple iMessages. ABDALLAH messages included, “Whore ass bitch,” “Indian whore,” and “you’re an Indian slut.” ABDALLAH also included MINOR 1’s parents in an iMessage group chat and messaged “worst muslim dad we’ve,” “ever seen,” and referred to MINOR 1 as a “whore.” ABDALLAH sent a picture of MINOR 1 and ABDALLAH together and a skull emoji.

38. As of August 26, 2024, ABDALLAH was still sending messages to MINOR 1 from multiple different numbers. A law enforcement officer advised ABDALLAH on August 27, 2024, and November 16, 2024, to cease communication with MINOR 1. ABDALLAH advised the officer that he continued to contact MINOR 1 because she was a child of Allah.

39. On December 21, 2024, ABDALLAH sent several offensive text messages from different numbers, including one from the “spoof” number reported as the number the December 23, 2024, USM bomb threat was made from, 587-205-6694. This message stated, “You will become a whore, Your father will become sick, Your police department will fall, Your life around you will fall.”

EMAILS FROM APPLE iCloud ACCOUNT

40. On January 3, 2025, USM received three emails to their business account from ahmadabdullahalmahdi@icloud.com. The first email stated, “I was never an Antichrist I am Christ I am the Holy Spirit You are all the embodiment of Satan I was always the innocent one just trying to get by now you all have to be punished for hurting a innocent man keep in mind this isn’t a threat of man this is a threat of god don’t fear me FEAR GOD.”

41. The second email stated, “Also since u guys are having a hearing on me how about you let me talk?? Probably not though you guys don’t like the good guy talking only you pig mouths.”

42. The third email stated, “usm will be an orphan home to house kids from the hoods of Milwaukee.”

43. Apple iCloud account ahmadabdullahalmahdi@icloud.com data was located in ABDALLAH’S cellphone. Also, based on the content of the messages, that the messages were sent to USM, the name on the account which is similar to ABDALLAH’s Instagram account, and the date of the messages, Affiant believes that ABDALLAH is the user for Apple iCloud account ahmadabdullahalmahdi@icloud.com.

EVIDENCE LIKELY POSSESSED BY APPLE

44. Based on my training and experience, I know that the iCloud is a cloud storage and cloud computing service that Apple provides to its customers and is accessible on the products, including the iPhone. Customers can use the iCloud to backup information, to include SMS and MMS messages, emails, photos, videos, music, calendars, third-party app data, and purchase history from Apple, that is captured and/or stored on their personal mobile device.

45. Based on my training and experience, I know that Apple customers may use the iCloud to back up their mobile devices, including iPhones, iPads and Macs, as a way to ensure that important information is not lost, as well as a means to save important information that is taking up too much space on their mobile device. It is also a way to ensure that when a mobile device is replaced—either for an upgrade or because the device has been lost, stolen, or damaged, the Apple customer can restore data to the new phone. Relatedly, I understand that items that may have been accidentally or intentionally deleted or otherwise unrecoverable from a device may remain in the iCloud account.

REQUEST TO MAINTAIN ACCOUNTS

46. Request to Maintain Account: I would further request the Court to order the Target Providers to continue to maintain the account(s) listed in Attachment A in an open and active status for one year from the date of this warrant so as not to disrupt this ongoing investigation.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

47. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Apple, Inc. Because the warrant will be served on Apple, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Apple account and iCloud account with username: ahmadabdullahmahdi@icloud.com, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered in Cupertino, CA.

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any emails, messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) February 21, 2025, Apple is required to disclose the following information to the government for each account listed in Attachment A:

a. The contents of all emails associated with the account from since account creation to current date, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

b. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

c. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple

and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

d. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

e. All records pertaining to the types of service used;

f. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §245(b)(2): Federally Protected Activities; 18 U.S.C. §875 (c): Interstate Threats; and 18 U.S.C. §1038(a): False Information and Hoaxes those violations involving Zidan Abdallah and occurring after August 1, 2024, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

A. Communications between the user of the SUBJECT ACCOUNT and victims;

B. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

C. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

D. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such persons(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO
FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. (“Apple”), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple’s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature